SOUTH AFRICAN RESERVE BANK

Draft directive in respect of issuing of electronic funds transfer credit payment instructions on behalf of the payer in the national payment system

Directive No. 1 of 2023

Contents

1. Definitions

1.1 Unless the context indicates otherwise where the interpretation should further be in the context of this directive, any word or expression used in this directive to which a meaning has been assigned in the National Payment System Act 78 of 1998, as amended (NPS Act), has that meaning.

1.2 **Beneficiary** refers to a person that is identified by the payer as the receiver of the funds associated with the electronic funds transfer credit.

1.3 **Clearing system participant** is a person defined as such in terms of section 1 of the NPS Act.

1.4 **Critical staff** means a natural person that performs functions that are essential to the operations of the juristic person issuing electronic funds transfer credit payment instructions on behalf of the payer using screen scraping, including a person who has access to information technology (IT) systems.

1.5 **Cyberattack** refers to the use of computer techniques by an attacker to take advantage of a weakness(es) related to IT systems, with the intent of causing damage on the information communication technologies (ICT) environment.

1.6 **Data breach** means a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data transmitted, stored or otherwise processed.

1.7 **Electronic funds transfer credit** means a payment instruction carried out by electronic means on behalf of a payer, with a view to making an amount of funds available to a beneficiary, irrespective of whether the payer and the beneficiary are the same person.

1.8 **Faster payments** refer to a low value credit-push payment service in which both the transmission of the payment message and the availability of funds

to the beneficiary occur in real time or near-real time, on a basis that the service is available 24 hours a day and 7 days a week (24/7).

1.9 **Fraud** refers to the issuing of a payment instruction with the intention to defraud a person.

1.10 **Front-end interface** is the point at which a payer interacts with a website or application.

1.11 **Governing body** refers to a person or body of persons, whether elected or not, that manages, controls and formulates the policy and strategy of the person issuing electronic funds transfer credit payment instructions on behalf of the payer using screen scraping, directs its affairs or has the authority to exercise the powers and perform the functions of the person issuing electronic funds transfer credit payment instructions on behalf of the payer using screen scraping.

1.12 **Informed consent** means any voluntary, specific and informed expression of will in terms of which permission is given by the payer for the processing of the payer's online banking credentials.

1.13 **Payer** is a person that issues a payment instruction.

1.14 **Payment instruction** is an instruction to transfer funds or make a payment, as defined in section 1 of the NPS Act.

1.15 **Person** refers to a natural or juristic person and includes a trust.

1.16 **Scheduled payment transaction** is a payment that is scheduled by the payer for a specific date as agreed between the payer and the beneficiary.

1.17 **Screen scraping** in payments means the use of computer techniques to access data from a clearing system participant's online banking website, with the use of the payer's online banking security credentials to issue an

electronic funds transfer credit payment instruction on behalf of the payer without the payer's informed consent.

1.18 **Sort-at-source** means the practice of sorting payment instructions based on multiple holders of destination accounts and submitting such payment instructions directly to the holders of the destination accounts or requesting clients to pay directly into specific accounts (e.g. third-party payment providers' or beneficiaries' accounts), resulting in the bypassing of the clearing system, which is undertaken through regulated acquiring or sponsoring relationships.

2. Background

2.1 In terms of section 10(1)(c) of the South African Reserve Bank Act 90 of 1989, as amended (SARB Act), the South African Reserve Bank (SARB) is required to perform such functions, implement such rules and procedures and, in general, take such steps as may be necessary to establish, conduct, monitor, regulate and supervise payment, clearing or settlement systems. Furthermore, the NPS Act provides for the management, administration, operation, regulation and supervision of payment, clearing and settlement systems in the Republic of South Africa, and for connected matters.

2.2 The national payment system (NPS) encompasses the entire payment process, from payer to beneficiary, and includes settlement between banks. The process includes all the tools, systems, instruments, mechanisms, institutions, agreements, procedures, rules or laws applied or utilised to effect payment. The NPS is a primary component of the country's monetary and financial system as it enables the circulation of money, assisting transacting parties to make payments and exchange value.

2.3 The SARB is empowered in terms of section 12 of the NPS Act to issue directives, after consultation with the payment system management body, to any person regarding a payment system or the application of the provisions of the NPS Act. Currently, the Payments Association of South Africa (PASA)

is recognised by the SARB in terms of section 3 of the NPS Act as a payment system management body to organise, regulate and manage its members in the payment system.

2.4 In recent years, the payment industry has witnessed the emergence of financial technology (fintech) companies that leverage technology to offer innovative tools, products and services. These tools, products and services are offered particularly in the e-commerce environment with minimal regulatory oversight. One such tool is screen scraping, which is used by a third party, usually a fintech company, in partnership with merchants, to conduct screen scraping to issue electronic funds transfer credit payment instructions for payments of goods and services online. Although screen scraping is popular in e-commerce payment transactions, it is now growing in usage in other payment activities such as bill payments, which are facilitated by a person that issues electronic payment instructions on behalf of payers.

2.5 Screen scraping exposes the NPS, including the participants and payers to risks such as those stipulated in paragraphs 2.5.1 to 2.5.7 below. Screen scraping requires the payer to share their online banking credentials with the person issuing the electronic funds transfer credit payment instruction on behalf of the payer, without the informed consent of the payer. These risks have a negative impact on the integrity, efficiency, security and confidence in the NPS. These risks include but are not limited to:

2.5.1 Lack of informed consent: Many payers that use the front-end interface of a person issuing electronic funds transfer credit payment instructions on behalf of the payer using screen scraping are not informed about the fact that by entering their online banking credentials they are not logging on to their actual clearing system participant's proprietary online banking platform. Instead, they are sharing their online banking credentials with a third party to issue electronic funds transfer credit payment instructions on their behalf. The use of payers' online banking credentials without their informed consent has a negative impact on the integrity of payments and security of the NPS.

2.5.2 Misleading conception that the payment is instant: A person issuing electronic funds transfer credit payment instructions on behalf of the payer using screen scraping usually markets its service as providing an 'instant or fast payment' to the beneficiary/merchant's account. This is misleading as a normal electronic funds transfer credit payment instruction does not necessarily result in the funds being credited into the beneficiary's account instantly unless the payer chooses the faster payments option to process the payment into the beneficiary's transactional account, or a transaction is an intrabank (on-us) transaction processed directly into the beneficiary's transactional account. Misleading payers and beneficiaries that the payment is instant undermines the integrity of payments, and confidence in the NPS.

2.5.3 Conducting sort-at-source: A person may use screen scraping to sort-at-source payments by using bank accounts from multiple banks to ensure that payments are on-us transactions, resulting in an 'instant' payment. Conducting sort-at-source negatively impacts the NPS as it goes against the SARB's objectives of promoting efficiency, safety, interoperability, modernisation and optimisation of interchange fees.

2.5.4 Lack of data privacy: Screen scraping puts payers' online banking credentials at risk of being compromised. Payers have no control over how their credentials, and any other data or personal information, are accessed, processed, used and stored by the third party (e.g. account numbers and account statements may be stored and utilised without the payer's knowledge or consent). This undermines the public's trust and confidence and security of the NPS.

2.5.5 Exposure to fraud: Rogue entities may pose as persons issuing electronic funds transfer credit payment instructions on behalf of the payer using screen scraping on fake e-commerce sites to capture payers' internet banking access credentials. Such entities may impersonate the payer and conduct any activity that the payer would have access to on their online banking platform (e.g. making real-time payments to themselves, applying for a personal loan, increasing transaction limits and ultimately initiating payments

to mule transactional accounts). Similar to a lack of data privacy, fraud weakens the public's trust, confidence, integrity and security of the NPS.

2.5.6 Breach of contractual agreements: By providing their online banking login credentials to a person issuing electronic funds transfer credit payment instructions on their behalf using screen scraping, payers might be in breach of their clearing system participant's terms and conditions. As a result, knowingly or unknowingly, payers might be relinquishing their rights of recourse and any legal protection in the event of fraud and/or subsequent loss. This would undermine the public's trust and confidence in the NPS.

2.5.7 Risk of financial loss or non-delivery of the goods/services purchased: Electronic funds transfer credit payments are final and irrevocable in nature, and payers may be unable to lodge disputes to reverse a transaction in the event of the e-commerce merchant not honouring their agreement (e.g. not delivering the goods or delivering incorrect or counterfeit goods). Payers might also be held liable for the interest payable on such amounts when payment was made from their credit card account or overdraft facilities. This would significantly and negatively impact the efficiency, integrity and security of the NPS.

3. Purpose

3.1 The purpose of this directive is to impose requirements on persons issuing electronic funds transfer credit payment instructions on behalf of the payer using screen scraping or any other tool in the NPS to mitigate the risks identified in paragraph 2.5 above.

4. Scope of this directive

4.1 This directive applies to any person issuing payment instructions on behalf of a payer using screen scraping or any other tool in the NPS.

5. Directive

5.1 Registration requirements

5.1.1 No person may issue electronic funds transfer credit payment instructions on behalf of a payer in the payment system unless that person:

a. is registered with the SARB in the manner and form prescribed by the SARB; and
b. has obtained informed consent of the payer prior to issuing such a payment instruction or initiating such a payment; or
c. has been exempted from registration by the SARB.

5.1.2 A juristic person may apply for registration with the SARB to issue payment instructions or initiate payment on behalf of a payer.

5.1.3 The application to register with the SARB must be addressed to the Head of the National Payment System Department at npsdirectives@resbank.co.za.

5.1.4 The application for registration must be accompanied by the following information and supporting documents:

a. proof of business registration and/or founding documents of a juristic or legal person, issued by the applicable competent South African authorities;
b. proof of physical address of the place of business in South Africa;
c. disclosure of ownership, including the names and certified copies of the identity documents of the shareholders, trustees and ultimate beneficial owners;
d. organisational structure;
e. the types and sources of funding, including the capital contribution for the establishment and operation of the business. In the case of a loan, the funding details of the name of the lender and their domicile must also be provided;
f. a reasonably measurable forecast budget calculation for the first three financial years which demonstrates that the applicant is able to employ

appropriate systems, resources and procedures to operate in a sound manner; and

g. a description of the applicant's governance arrangements and internal control mechanisms relating to, inter alia, administrative, risk management and accounting procedures, which demonstrates that these governance arrangements, control mechanisms and procedures are appropriate, sound and adequate.

5.2 Conditions for registration

5.2.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. employ or appoint a key person(s) responsible to ensure compliance with the relevant legislation, rules, regulatory frameworks and agreements;
b. ensure that the key person(s) is competent, qualified, experienced and skilled to execute the compliance function;
c. be satisfied that the key person(s) is honest and has integrity;
d. furnish the SARB with the curriculum vitae and copies of supporting documents, including but not limited to the identity document, proof of physical address and certificates of qualifications of a key person(s) upon their appointment;
e. have clear and transparent policies and procedures approved by its governing body for on-boarding merchants;
f. have terms and conditions approved by its governing body for the use of its service by merchants and payers. The terms and conditions must be objective, non-discriminatory and proportionate;
g. ensure that contractual agreements with merchants and the terms and conditions for payers clearly state that the party responsible for a fraudulent or unauthorised or incorrectly issued electronic funds transfer credit payment instruction must bear the risk;
h. satisfy the SARB that it has the necessary processes and systems in place to secure the payer's data and online banking credentials to mitigate risks of fraud and cyberattacks; and

i. perform due diligence on merchants with whom it enters into partnership arrangements, including the following:
    i. verification of the true identity of the merchant;
    ii. establishment of whether the merchant's business is legal and/or registered with the relevant authorities;
    iii. understanding the business activity of a merchant; and
    iv. regular monitoring of merchant's transactions.

5.2.2 The SARB reserves the right to decline an application for registration if the requirements in this directive are not met.

5.3 Ongoing obligations

5.3.1 Marketing

5.3.1.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. comply with responsible marketing requirements of its product or service to payers as provided for in the Code of Advertising Practice as governed by the Advertising Regulatory Board; and
b. refrain from using any clearing system participant's branding on its front-end interface or when marketing its services unless it is authorised in writing by the said clearing system participant.

5.3.2 Consumer awareness

5.3.2.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. where it has partnered with a clearing system participant, inform its merchants and payers explicitly and clearly of such a partnership;
b. publicly disclose, in simple language, terms and conditions for using its product or service, procedures for handling payer complaints, privacy policy, and other terms and conditions; and

c. Must refrain from misleading payers that transactions are compliant with standards that apply to electronic funds transfer credit payments.

5.3.3 Informed consumer consent

5.3.3.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must obtain informed payer consent prior to using the payer's online banking credentials to access the transactional accounts of the payer to issue an electronic funds transfer credit payment instruction on behalf of the payer.

5.3.3.2 The request for informed consent by the person issuing electronic funds transfer credit payment instructions on behalf of the payer using screen scraping must:

a. be simple and clear to the payer;
b. state that by entering their login credentials, the payer is sharing the credentials with that person and is not logging on to their online banking website or app; and
c. state that the payer is authorising that person to use their online banking credentials to issue the electronic funds transfer credit payment instruction on their behalf and that such details shall be used only for that purpose.

5.3.3.3 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must request the payer informed consent to share their login credentials for each electronic funds transfer credit payment instruction, including scheduled payment transactions.

5.3.4 Operational risk

5.3.4.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. have sound and effective policies, systems and procedures to mitigate operational risks, including the risks it directly bears from or poses to its

merchants, its customers, clearing system participants facilitating or enabling electronic funds transfers and/or any other relevant entities;

b. have mechanisms to promptly respond to, resolve and remedy any data breaches, transmission errors, unauthorised access and fraud;
c. have a comprehensive cyber-incident management plan approved by the IT function and its governance structures; and
d. carry out regular and comprehensive security risk assessments of its critical staff, IT systems and business process environment to identify, assess and mitigate inherent risk exposures.

5.3.5 Payer data protection

5.3.5.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. comply with data processing requirements as provided for in the personal data protection laws, including but not limited to the Protection of Personal Information Act 4 of 2013 (POPI Act);
b. issue an electronic funds transfer credit payment instruction only when the payer has made an instruction for the amount in question and not modify the amount, the beneficiary or any other detail of the transaction;
c. encrypt the payer's online banking credentials at the time when the payer enters the credentials on its front-end interface platform;
d. use the latest and most robust encryption standards to secure the payer's credentials in transit;
e. use and regularly update anti-virus software to protect its system from malware and data security breaches;
f. not store payers' online banking credentials and other sensitive payer payment data within its database or systems;
g. only use the online banking credentials for screen scraping on behalf of the payer and safely destroy the payers' online banking credentials immediately after executing a payment; and
h. have adequate information and data security infrastructure and systems to prevent, detect and resolve any possible unauthorised access to the online banking of the payer and/or data breach.

5.3.6 Dispute resolution mechanism

5.3.6.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. have a fair and formal dispute resolution mechanism that provides merchants, clearing system participants and payers with practical means to lodge and resolve disputes relating to the issuing of electronic funds transfer credit payment instructions on behalf of the payer, including but not limited to instances of fraud, failure by merchants to honour purchase orders, unpaid orders or failed payments after the merchant has already delivered the goods/services and possible data breaches;
b. ensure that its dispute resolution mechanism, including the complaints handling facility is clearly and easily accessible to payers and merchants through all applicable communication channels such as a phoneline, email, mobile devices and a website;
c. ensure that the dispute resolution mechanism does not contravene the settlement provisions as stipulated in section 5 of the NPS Act; and
d. appoint an officer(s) responsible for the regulatory and payer complaints handling functions who shall:
    i. promptly respond to all complaints raised and resolve the matter within a reasonable timeline.

5.3.7 Traceability, audit and record keeping

5.3.7.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. have systems that ensure that each transaction is traceable, from authorisation using the payer's online banking credentials until the merchant is notified about the payment;
b. have a robust internal and external audit function that will undertake an assessment of the effectiveness of that person's risk-management and control processes;

c. be able to demonstrate, when requested by the SARB, that it applies robust data security standards, including its data encryption;
d. keep the information obtained during its onboarding process pertaining to a merchant or prospective merchant throughout its business relationship and for at least five years from the date on which the business relationship is terminated; and
e. keep a record of every transaction, whether the transaction is a once-off transaction or repeated transaction for at least five years from the date on which that transaction is concluded. A transaction record must at a minimum include the amount involved, the date on which the transaction was concluded, the parties to the transaction and the nature of the transaction.

5.3.8 Liability risk management

5.3.8.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:
a. have an insurance or guarantee mechanism against possible losses for payers, merchants and clearing system participants;
b. not mislead payers or merchants in believing that the issued electronic funds transfer credit payment instruction will be credited instantly to the merchant's account unless the real time payment option is used to process the payment directly into the merchant's transactional account or a transaction is an intrabank transaction processed directly into the merchant's transactional account;
c. have an effective mechanism to detect and identify incidents of fraudulent or unauthorised or incorrectly issued electronic funds transfer credit payment instructions and conduct reviews of audit trails to identify the source of the incident in order to determine the party liable for losses;
d. prove that, where a payer denies having authorised a payment instruction, the informed payer consent or authorisation was obtained from the payer, with the accurate payment amount and accurate beneficiary name and transactional account number and that the

payment was not affected by technical deficiencies within its systems; and

e. pay a refund where it bears the liability or responsibility for fraudulent, unauthorised or incorrectly facilitated transactions to the payer within a reasonable time through the original method of payment, unless specifically agreed by the payer to have the credit processed through an alternate mode.

5.3.9 Attestation of compliance

5.3.9.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must have an audit function or appoint a qualified internal auditor to attest to the declaration of compliance with this directive, twice a year.

5.3.9.2 The attestation of compliance referred to in paragraph 5.3.9.1 must be sent to the SARB by 31 March and 30 September each year using the following email address: npsdirectives@resbank.co.za.

5.3.10 Reporting requirements

5.3.10.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. submit to the SARB its monthly data on volumes and values of transactions processed on or before the 15th of every month, using the email address in paragraph 5.3.9.2 above; and

b. report data security incidents (data breach, cyberattack, fraud and so on) to the SARB immediately after being made aware of such incident and provide an analysis of the root cause and preventive measures undertaken to prevent recurrence, using the email address in paragraph 5.3.9.2 above.

6. Inspection

6.1 The SARB may conduct an independent inspection on a person issuing electronic funds transfer credit payment instructions on behalf of the payer in the form and manner determined by the SARB to establish compliance with this directive by that person.

6.2 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must produce to the SARB officials, all documents or information, relevant for this directive, upon request by such officials.

6.3 In case of suspected non-compliance, malpractice or fraud, the SARB official may seize documents and records, relevant for this directive, from the affected party.

7. Effective date and non-compliance

7.1 The directive is effective 90 days after publication thereof. The SARB reserves the right to amend any requirements in this directive.

7.2 A person issuing electronic funds transfer credit payment instruction on behalf of the payer must comply with the requirements or conditions as stipulated in this directive.

7.3 Contravention of this directive is an offence in terms of section 12(8) of the NPS Act.

7.4 The SARB may terminate the registration of a person registered in terms of this directive where such person fails to comply with this directive, or if it is in the interest of safety and efficiency of the NPS.

7.5 Prior to terminating a registration, the SARB shall issue a notice of its intention to terminate the registration and give that person reasonable time to remediate the deficiencies identified. The time provided to remediate the deficiencies shall be determined on a case-by-case basis.

8. Conclusion

8.1 If a person issuing an electronic funds transfer credit payment instruction on behalf of the payer is uncertain as to whether its current or future business practices are aligned with this directive, that person should initiate discussions with the SARB to clarify the matter.

8.2 Attestation of compliance as well as any enquiry or clarification concerning this directive should be sent to the following email address: npsdirectives@resbank.co.za.

9. Comments and contact details

9.1 Stakeholders and other interested parties are invited to forward their comments on this draft directive by 23 June 2023. Comments should be addressed to npsdirectives@resbank.co.za.